

REMARKS

The Office Action of December 13, 2005 has been reviewed, and in view of the following remarks, reconsideration and allowance of all of the claims pending in the application are respectfully requested. Although Applicants do not agree with the Examiner's contentions, independent claims 1, 8 and 15 have been amended in an effort to expedite prosecution of the present application. No new matter has been added.

I. REJECTIONS UNDER 35 U.S.C. § 102

Claims 1-20 currently stand rejected under 35 U.S.C. § 102(e) as being allegedly anticipated by U.S. Patent No. 6,453,353 to Win *et al* ("Win"). The Office Action alleges that each and every claimed limitation is shown by Win. Applicants respectfully disagree.

A. Win fails to disclose each and every claim limitation

Win purports to disclose a network using role-based navigation among protected information resources (col. 1, lines 11-15). More specifically, Win appears to discuss a method and apparatus for controlling access to protected information resources by enabling organizations to register information sources and user information in a central repository (col. 5, lines 12-14). Win purports to allow administrators to implement access rules by defining roles that users play when working for an organization or doing business with an enterprise, thus forming an additive data model (col. 5, lines 21-23, 57-58).

Embodiments of the claimed invention are directed to integrating security and user account data with remote repositories and validating the identity of the user through authentication. In addition, access control may be implemented to determine what the user may be allowed to see, do or access, once the user has been identified to the system. Access control may include privileges and permissions. Privileges may define the types of actions that particular users and groups may

perform in the system. Permissions may define which users and groups have access to what objects and the degree to which the user may access those objects. *See* Specification at page 27, lines 16-20.

For example, when a server command is requested, the server may check certain access rights to determine if a particular command may be executed. In general, the server may check access rights on a Server Definition object, for example, that may be used to initialize the server at startup. This allows the user to have different capabilities on different servers within the same system. *See* Specification at page 29, lines 3-8. Furthermore, the present invention provides security and user account integration with remote authentication servers or remote repositories located within a server different than that of a server of the reporting system. *See* Specification at page 2, lines 13-14.

According to an embodiment of the claimed invention, a method for integrating security and user account data comprises “enabling a user to submit user credential input to a reporting system;” “identifying an authentication process;” “forwarding the user credential input to a first server;” and **“enabling the first server to apply the authentication process to authenticate the user against a remote repository for verifying the user credential input and to determine user access control data for identifying at least one user privilege for performing one or more actions and at least one user permission associated with one or more objects, wherein the remote repository is located within a second server, the second server being different from the first server.”**

The disclosure of Win fails to show at least the limitation directed to **“enabling the first server to apply the authentication process to authenticate the user against a remote repository for verifying the user credential input and to determine user access control data for identifying at least one user privilege for performing one or more actions and at least one user permission**

associated with one or more objects, wherein the remote repository is located within a second server, the second server being different from the first server”, as expressly recited independent claim 1, and similarly recited in independent claims 8 and 15 (emphasis added). On the other hand, Win discloses – as evidenced by an excerpt cited by the Examiner – that a role-specific access menu to a network user that is available to show only those resources that the user is authorized to access according to the user's profile information, including roles and privileges:

FIG. 5E is a state diagram of a method delivering a role-specific access menu to a network user. In the preferred embodiment, after the Authorization service of Authentication Client module 414 has looked up a user's roles from the Registry Server 108, Access Menu Module 412 uses a Personalized Menu Service *to build a list of resources* 208 that are available to the user. As shown by state 538, Access Server 106 determines that the user is authentic, using the steps described above, and requests Registry Server 108 to return a profile of the user. In state 540, Registry Server 108 returns profile information for the user to Access Server 106. In response, the Personalized Menu Service constructs *a personalized menu of resources showing only those resources* that the user is authorized to access according to the user's profile information, including the user's roles and privileges.

See Win at col. 11, lines 42-57.

Furthermore, the invention of Win – as evidenced by an excerpt relied upon by the Examiner – appears to be directed to enabling organizations to register information sources and user information in a central repository rather than a remote repository that is not owned by the server:

The system 2 enables organizations to register information sources or Resources and register Users of the information in a central repository. A Resource is a source of information, identified by a Uniform Resource Locator (URL) and published by a Web server either in a static file formatted using Hypertext Markup Language (HTML) or in a dynamically generated page created by a CGI-based program. Examples of resources include a Web page, a complete Web site, a Web-enabled database, and an applet.

See Win at col. 5, lines 12-20.

As a result, Applicants respectfully submit that Win does not disclose each and every limitation, feature, or functionality of the claimed invention. Applicants respectfully submit that Win makes no mention of applying the authentication process to against “a remote repository” and “wherein the remote repository is located within a second server, the second server being different from the first server.” In fact, Win appears to merely disclose that resource and user information are organized in a central repository. This is clearly distinguishable from a remote repository that is not owned by the server. Furthermore, even assuming that Win teaches a remote repository, Applicants respectfully submit that Win fails to disclose the step of determining user access control data for identifying at least one user privilege for performing one or more actions and at least one user permission associated with one or more objects. In fact, Win appears to merely disclose a role-specific access menu to a network user that is available to show only those resources that the user is authorized to access according to the user’s profile information, including roles and privileges. This is clearly distinguishable from access control data for identifying at least one user privilege for performing one or more actions and at least one user permission associated with one or more objects.

As a result, the disclosure of Win fails to disclose or show at least the limitation directed to “enabling the first server to apply the authentication process to authenticate the user against a remote repository for verifying the user credential input and *to determine user access control data for identifying at least one user privilege for performing one or more actions and at least one user permission associated with one or more objects, wherein the remote repository is located within a second server, the second server being different from the first server.*” These features are simply not disclosed or even contemplated by Win. For a proper rejection under 35 U.S.C. §

102(e), each and every claim limitation must be shown in a single reference. The Office Action has failed to meet this requirement and thus the rejection is unsupported and should be withdrawn.

B. Dependent claims

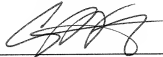
Dependent claims 2-7, 9-14 and 16-20 depend from either independent claims 1, 8 and 15, respectively. As such, each of these dependent claims contain each of the features recited in the independent claims. For the reasons stated above, Win fails to disclose the claimed invention and therefore the rejections should be withdrawn.

CONCLUSION

It is respectfully submitted that this application and all pending claims are in condition for allowance and such disposition is earnestly solicited. If the Examiner believes that prosecution and allowance of the application will be expedited through an interview, whether personal or telephonic, the Examiner is invited to telephone the undersigned with any suggestions leading to the favorable disposition of the application.

The Director is hereby authorized to treat any current or future reply, requiring a petition for an extension of time for its timely submission as incorporating a petition for extension of time for the appropriate length of time. Applicants also authorize the Director to credit and differences or overpayment of fees to the undersigned's Deposit Account No. 50-0206.

Respectfully submitted,



George Wang
Registration No. 58,637

For: Brian M. Buroker
Registration No. 39,125

Hunton & Williams LLP
1900 K Street, NW
Washington, D.C. 20006-1109
(202) 955-1500 (phone)
(202) 778-2201 (facsimile)

Date: July 6, 2006